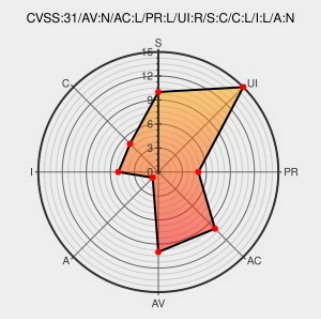
CVE-2023-4382

Published on: Not Yet Published

Last Modified on: 08/22/2023 10:18:00 PM UTC

CVE-2023-4382

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Hyip Rio from Tdevs contain the following vulnerability:

A vulnerability, which was classified as problematic, has been found in tdevs Hyip Rio 2.1. Affected by this issue is some unknown functionality of the file /user/settings of the component Profile Settings. The manipulation of the argument avatar leads to cross site scripting. The attack may be launched remotely. VDB-237314 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.

CVE-2023-4382 has been assigned by cna@vuldb.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **tdevs** - **Hyip Rio** version **= 2.1**

CVSS3 Score: 5.4 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVE References

Description	Tags	Link
CVE-2023-4382: tdevs Hyip Rio Profile Settings settings cross site scripting	vuldb.com text/html	MISC vuldb.com/?id.237314
Login required	vuldb.com text/html Inactive Link Not Archived	MISC vuldb.com/?ctiid.237314
Hyip Rio 2.1 Cross Site Scripting / File Upload ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/174212/Hyip-Rio-2.1-Cross-Site-Scripting-File-Upload.html

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tdevs	Hyip Rio	2.1	All	All	All

cpe:2.3:a:tdevs:hyip_rio:2.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report